

UNITED STATES DISTRICT COURT

for the
Western District of Washington

FILED	LODGED
RECEIVED	
12/18/2020	
CLERK U.S. DISTRICT COURT	
WESTERN DISTRICT OF WASHINGTON AT TACOMA	
BY	DEPUTY

In the Matter of the Search of
*(Briefly describe the property to be searched
or identify the person by name and address)*
Apple ID: goodealjohnmneal@gmail.com,
Described more fully in Attachment A, attached
hereto

Case No. 3:20-mj-05293

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE ATTACHMENT A, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, ATTACHED HERETO AND INCORPORATED HEREIN BY REFERENCE.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.


The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. § 841(a)(1)	Distribution of, and Possession with Intent to Distribute, Controlled Substances
21 U.S.C. § 333(i)(3)	Distribution of Counterfeit Drugs

The application is based on these facts:

- ☒ See Affidavit of DEA SA Colin M. Fine.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☒ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

DEA Special Agent Colin Fine

Printed name and title

- ☐ The foregoing affidavit was sworn to before me and signed in my presence, or
- ☒ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 12/18/2020


Judge's signature

City and state: Tacoma, Washington

Theresa L. Fricke, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT OF COLIN M. FINE

STATE OF WASHINGTON)
) SS
COUNTY OF PIERCE)

I, Colin M. Fine, being first duly sworn on oath, depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am an “investigative or law enforcement officer of the United States” within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

2. I am a Special Agent with the Drug Enforcement Administration (DEA), United States Department of Justice, and have been so employed since April 2017. In that capacity, I investigate violations of the Controlled Substances Act (Title 21, United States Code, Section 801, et seq.). I am currently assigned to the Seattle Field Division, Tacoma Resident Office.

3. My training and experience include, but are not limited to, a twenty-week course at the DEA academy in Quantico, Virginia. At the DEA academy, I was trained in all aspects of conducting narcotics investigations to include debriefing defendants, witnesses, and informants, conducting surveillance, executing search warrants, conducting controlled deliveries, utilizing law enforcement, open source, and social media databases, and seizing narcotics and narcotics-related assets. Prior to my employment with DEA, I served 12 years on active duty in the United States Marine Corps, achieving the rank of Gunnery Sergeant.

4. During the course of my law enforcement career, I have become familiar with investigations of drug trafficking organizations, methods of importation and exportation, distribution, and smuggling of controlled substances, and financial and money laundering investigations. I have participated in investigations involving

1 organizations trafficking in controlled substances, including heroin, and such
2 investigations have resulted in the arrests of drug traffickers and seizures of controlled
3 substances. I have participated in the execution of drug search warrants and have
4 personally been involved in the seizure of controlled substances. Based on my training,
5 experience and conversations with other experienced narcotics investigators, I have
6 gained experience in the techniques and methods used by drug traffickers to distribute
7 controlled substances.

8 5. The facts set forth in this affidavit arise from my personal and direct
9 participation in the investigation, my experience and training as a DEA Special Agent,
10 my conversations with witnesses and other law enforcement personnel participating in
11 this and related investigations, and my review of relevant documents and reports. I have
12 not included each and every fact known to me or other investigative personnel
13 concerning this investigation.

14 **SOURCES OF INFORMATION**

15
16 6. I make this affidavit based upon personal knowledge derived from my
17 participation in this investigation and upon information I believe to be reliable from
18 various sources, including:

19 a. My training and experience investigating drug trafficking and related
20 criminal activity, as described above;

21 b. Oral and written reports and documents about this and other
22 investigations that I have obtained from agents of the DEA and the Joint Narcotics
23 Enforcement Team (JNET), and other federal, state and local law enforcement agencies;

24 c. Physical surveillance conducted by the aforementioned agencies,
25 and other law enforcement agencies, that has been reported to me directly or indirectly;

26 a. Telephone toll records, pen register and trap and trace information,
27 and subscriber information;

28 b. Washington State Department of Licensing records;

- c. Commercial databases;
- d. Public records; and
- e. Publicly viewable information on social media websites (*i.e.*, Facebook and Instagram).

6. Since this affidavit is being submitted for the limited purpose of seeking authorization for the above requested search warrant, I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are essential to establish the necessary foundation for a fair determination of probable cause to support the Application.

7. In the following paragraphs, I describe communications between various individuals. Except where specifically indicated with quotation marks, the descriptions are summaries of the conversations and are not meant to reflect the specific words or language used.

PURPOSE OF AFFIDAVIT

8. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc. ("Apple") to disclose to the government copies of the information, including the content of communications, associated with the Apple ID gooddealjohnmcneal@gmail.com (the "SUBJECT ACCOUNT"), that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

9. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe that JOHN L. MCNEAL JR., and others, have committed violations of Distribution of, and Possession with Intent to Distribute, Controlled Substances, in violation of 21 U.S.C. § 841(a)(1)(heroin and methamphetamine); and Distribution of Counterfeit Drugs, in violation of 21 U.S.C. § 333(i)(3)(counterfeit Oxycodone pills containing fentanyl), as described herein. There is

also probable cause to search the SUBJECT ACCOUNT for information described in Attachment A for evidence, fruits, and instrumentalities of these crimes and items to be seized listed in Attachment B.

JURISDICTION

10. This court has jurisdiction to issue the proposed warrant because it is a “court of competent jurisdiction” as defined in 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offenses being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

I. Summary of Investigation

11. As described herein, the DEA and JNET are investigating JOHN MCNEAL JR. as a methamphetamine and heroin dealer within the Western District of Washington. In November 2019, law enforcement searched MCNEAL’s residence after obtaining a search warrant from Lewis County Superior Court. During the search, law enforcement located approximately 170 grams of methamphetamine, approximately 80 grams of heroin, and approximately 5 ounces of a white powder suspected to contain fentanyl. MCNEAL is currently pending felony charges in Thurston County.

12. In July 2020, MCNEAL was observed by law enforcement selling heroin to a Confidential Source¹. During this controlled purchase, MCNEAL utilized phone number (360) 580-0893. As investigators continued the investigation into MCNEAL, investigators identified at least five of MCNEAL’s customers and seized approximately five ounces of heroin collectively from those five customers. All five customers made post-Miranda statements identifying MCNEAL as their only source of supply for drugs.

//

¹ The CS utilized during this controlled buy is no longer used as a CS. During the controlled buy, the CS took a portion of the heroin for themselves. When confronted by investigators with this fact, the CS admitted to doing so, and was subsequently deactivated as CS. During the controlled purchase the CS and MCNEAL were audio/video recorded as well as directly observed by investigators throughout the duration of their encounter.

13. In August 2020, one of MCNEAL's customers, L.B., sold heroin to Bradley Economou in Chehalis, WA. Within hours of that transaction, Bradley Economou was found dead by his brother. Following an autopsy, the forensic pathologist listed Economou's cause of death as acute heroin intoxication.

14. On October 8, 2020, MCNEAL was arrested within Lewis County while in possession of approximately 444 grams of heroin, pills suspected to contain fentanyl, and methamphetamine. MCNEAL is currently facing related charges in Lewis County.

II. Controlled Substance Homicide Investigation

15. Following the death of Bradley Economou, the Lewis County Sheriff's Office obtained search warrants for L.B.'s Facebook account and for Bradley Economou's phone. The search of L.B.'s Facebook account and Bradley Economou's phone confirmed the following: On the evening of August 3rd, 2020, Bradley Economou contacted L.B., one of MCNEAL's known customers, via Facebook messenger, and ordered heroin to be delivered to him. L.B. agreed to sell him heroin and met him near his residence in Chehalis, WA. According to Facebook messages recovered from a WA State search warrant of Bradley Economou's Facebook, this meeting ultimately took place at approximately 7:40pm on August 3, 2020.

16. On August 4, 2020, around 11:00am, Bradley Economou was found dead by his brother, Brett Economou. Brett Economou told law enforcement that his brother is a heroin and methamphetamine user. Brett Economou stated to the best of his knowledge Brad had used heroin the previous night around 8:30pm. Brett stated Brad normally injects heroin and is very sensitive to it. Brett mentioned that he had to use Narcan to revive Brad two nights prior². Brett said that at approximately 8:00am that morning, he checked on Brad inside his bedroom. Brett stated he believed Brad was sleeping and did not try to wake him up. Brett said when he checked on Brad, just prior to call 911, Brad

² Narcan, also known as Naloxone, is a nasal spray medication designed to rapidly reverse opioid overdose. According to drugabuse.gov it can very quickly restore normal respiration to a person whose breathing has slowed or stopped as a result of overdosing with heroin or prescription opioid pain medications.

1 was “stiff.” Brett said after calling 911, he used Narcan again and began chest
2 compressions. The cause of death was determined to be acute heroin intoxication.

3 17. Upon learning of Brad Economou’s death, L.B. told at least two JNET
4 confidential sources of her involvement, specifically that she sold Bradley Economou
5 heroin the day that he died. L.B. also told these confidential sources that she changed her
6 Facebook name after this event and was directed by B.H., her intimate partner, to delete
7 any mention of the events leading up to the death of Bradley Economou that would link
8 her, B.H., or MCNEAL to the transaction or the death. B.H. would later tell investigators
9 that he was directed by MCNEAL to delete information from his phone linking
10 MCNEAL to Brad Economou’s death.

11 18. On September 21, 2020, investigators conducted surveillance on L.B. and
12 B.H. in Lewis County and observed the pair depart their hotel room and meet with at
13 least three known drug users to conduct what appeared to investigators to be drug sales.
14 L.B. and B.H. would conduct a short meeting, then use their phones before relocating to a
15 nearby parking lot for the next short meeting. They would then repeat this process.
16 Investigators contacted and detained L.B. and B.H. while they were in their vehicle.
17 Following a K9 alert to their vehicle, L.B. and B.H. consented to a search of the vehicle
18 and their hotel room where law enforcement located approximately one to two ounces of
19 heroin, scales, and packaging material.³

20 19. During separate Post-Miranda interviews, B.H. and L.B. each stated that
21 the heroin located within their vehicle had come from MCNEAL within the past day.
22 B.H. and L.B. each stated MCNEAL was their only source for drugs. B.H. said that as he
23 was being arrested, he sent a text message to MCNEAL that he was going to jail.
24

25
26 ³ Officer Stephen Summers’ assigned K9 ‘Samson’ has been a certified narcotics detection K9 since April 3, 2020,
27 being specifically trained to detect the odor of illegal narcotics, specifically methamphetamine, cocaine, and heroin,
28 after completing over 200 hours of training per Washington Administrative Code (WAC) 139-05-0915.
Certification was completed by the California Narcotics Canine Association and the Washington Criminal Justice
Training Center (CJTC). Current certifications under CJTC standards are valid for 24 months.

1 MCNEAL responded, "Ok, delete." B.H. explained that this was a pre-arranged failsafe
2 between him and MCNEAL, to alert MCNEAL to law enforcement's presence and for
3 MCNEAL to begin to gather bail money for B.H. B.H. stated the MCNEAL had
4 previously bailed another local drug trafficker (R.J.) out of jail following a narcotics
5 arrest by JNET investigators in Lewis County. Through jail calls and information
6 provided by confidential sources, investigators believe that MCNEAL posted bail for R.J.
7 when he was arrested by JNET earlier in the year.

8 20. B.H. also told investigators that MCNEAL was his (B.H.'s) only source of
9 supply, and that he was loyal to MCNEAL. B.H. said the heroin L.B. gave to Bradley
10 Economou, which he believes resulted in Economou's death, came from MCNEAL.

11 21. Additionally, B.H. stated to investigators that following the death of
12 Bradley Economou, B.H. and MCNEAL had a phone conversation in which MCNEAL
13 directed B.H. to delete any and all messages that would link the pair to the death of
14 Bradley Economou. B.H. said that MCNEAL told B.H. that he (meaning MCNEAL)
15 would do the same and that L.B. should also delete her electronically stored messages.
16 Through previous search warrant applications, and statements from L.B. and B.H.,
17 investigators know that the pair talked to MCNEAL through text messages, phone calls,
18 and through Facebook messenger. In the days leading up to and subsequent to
19 Economou's death, investigators noted a complete lack of communications between
20 MCNEAL, L.B. and B.H.. This lack of communication is consistent with L.B. and B.H.
21 deleting their communications at MCNEAL's direction. Investigators have noted that
22 L.B. went as far as also changing her Facebook display name following the death of
23 Bradley Economou, although she later claimed during her interview that the name change
24 was due to a family dispute.

25 **A. Arrest of MCNEAL in October 2020**

26 22. On October 7, 2020, L.B. and B.H. advised investigators that MCNEAL
27 had contacted them through phone number (360) 508-0893, the phone number known to
28

1 law enforcement to be utilized by MCNEAL.⁴ They stated that MCNEAL had agreed to
2 deliver the pair one to two ounces of heroin, and that MCNEAL would be traveling from
3 the Shelton area to Centralia. While waiting for MCNEAL to arrive, investigators
4 conducted surveillance on L.B. and B.H. because information had been provided that
5 L.B. and B.H. were still selling heroin. During this surveillance, investigators observed
6 L.B. and B.H. conduct a drug transaction to known users. When investigators contacted
7 L.B. and B.H, they located approximately 20.7 grams of heroin contained inside a
8 hairbrush with a screw off cap, four grams of heroin from L.B.'s person, and 9.4 grams
9 methamphetamine from inside L.B. and B.H's vehicle. L.B. and B.H. stated that they
10 received the heroin from MCNEAL in the early hours of October 7, 2020. Investigators
11 instructed L.B. and B.H. to return to their hotel room and maintain contact with
12 investigators. L.B. and B.H. followed the instructions and provided updates to
13 investigators about MCNEAL's whereabouts.

14 23. Shortly after midnight on October 8, 2020, L.B. and B.H. informed
15 investigators that MCNEAL would be traveling to their location to conduct the one to
16 two-ounce heroin delivery. Within minutes, investigators located MCNEAL driving in
17 his known vehicle and conducted a traffic stop on his vehicle. Following a K9 alert to
18 MCNEAL's vehicle, investigators obtained a search warrant and subsequently seized
19 approximately 444 grams of heroin and approximately 8 grams of counterfeit blue pills
20 stamped M-30 suspected to contain fentanyl⁵. Also seized during this search warrant was
21 MCNEALs cellphone, an iPhone.

22 //

23 _____
24 ⁴ The x0893 number is subscribed to J.S. out of Centralia, WA. During a search of MCNEAL's iPhone subsequent
25 to his arrest, communication between J.S. and MCNEAL suggest that MCNEAL and J.S. share a phone account and
26 that MCNEAL is responsible for paying at least a portion of the amount due. J.S. and MCNEAL are known to law
27 enforcement to be longtime close friends.

28 ⁵Officer Ruben Ramirez assigned K9 'Pax' has been a certified narcotics detection K9 since June 27, 2018, being
specifically trained to detect the odor of illegal narcotics, specifically methamphetamine, cocaine, and heroin, after
completing over 200 hours of training per Washington Administrative Code (WAC) 139-05-0915. 'Pax' completed
recertification training on July 17, 2019 by the California Narcotics Canine Association and the Washington
Criminal Justice Training Center (CJTC). Current certifications under CJTC standards are valid for 24 months.

B. Search of MCNEAL's iPhone

24. Following MCNEAL's arrest in October 2020, JNET investigators applied for and were granted a Centralia Municipal Court search warrant for the iPhone in MCNEAL's possession at the time of his arrest. This phone was the x8093 number which was also utilized during the earlier mentioned controlled purchase, during which MCNEAL was overhead on the audio/video recording device on a phone call to a third party about the pending sale of a vehicle where MCNEAL provides his name and phone number.

25. During an extraction of data from the phone investigators located text communications between MCNEAL and B.H. from only October 6 through October 8, 2020. Those messages begin with B.H. asking MCNEAL to meet up so that B.H. could acquire heroin and methamphetamine to sell to B.H.'s customers. The communications indicate that MCNEAL and B.H. met around 4:00am on the morning of October 7, 2020, and B.H. received approximately one ounce of heroin and a small amount of methamphetamine. The amount described in the communications is consistent with what investigators later seized from L.B. and B.H. on October 7, 2020.

26. On October 8, 2020, at 4:11am, MCNEAL sends the following message to B.H.: "You guys should really think about switching rooms with JNet out being so active lately and remember your next sentence is going to be probably 3 times longer then [sic] the last"[.] After B.H. tells MCNEAL that he and L.B. will switch rooms, the next communication between MCNEAL and B.H. begins at 7:00pm the same day. B.H. asks MCNEAL to meet up to sell B.H. one and half ounces of heroin. MCNEAL agrees to meet with B.H., which results in MCNEAL'S arrest.

27. Also, during the extraction of data from MCNEAL'S iPhone, investigators located the email address, gooddealjohnmneal@gmail.com, associated with the iCloud SUBJECT ACCOUNT, and noted that there were numerous daily communication files and records data dating back to January 25, 2020, and Facebook messenger communications dating from May 25, 2019, to his October 2020 arrest. Most of the

1 stored text messages between January 25, 2020, and August 11, 2020, are between
 2 MCNEAL and his children's mother, and MCNEAL and his current girlfriend. After
 3 August 11, 2020, a week after Bradley Economou's death, investigators noted the records
 4 showed MCNEAL's communications with his drug customers resumed. Specifically,
 5 MCNEAL used Facebook messenger on his phone daily to arrange drug purchases with
 6 at least ten customers. A sample exchange of these messages included this Facebook
 7 message string on September 7, 2020:

8 K.G.: When can you get blues

9 MCNEAL: I have them

10 MCNEAL: But need 20 each

11 K.G.: Oh great, I can probably swing 20 might know someone willing to pay 25-
 12 30\$, let me double check before I say for sure how many you got

13 K.G.: How many you got

14 K.G.: Ill sell all those blue

15 MCNEAL: Ok

16 MCNEAL: I got like 100 of them right now

17 K.G.: I got fifty sold for sure

18 K.G.: Kay got another 15 sold, when can I get them. I can meet all three before
 19 2pm

20 MCNEAL: Tomorrow before I go to court at 130 some time cuz I'm in Tacoma
 21 still

22 28. Based upon my training and experience, I know that in this context when
 23 MCNEAL and K.G. reference "blue" that they are referring to counterfeit Oxycodone
 24 blue pills stamped M-30 that contain fentanyl. The following day, MCNEAL has a
 25 conversation with K.G. where he said that his court case in Thurston County was
 26 continued due to the current COVID-19 pandemic.

27 29. The messages also show MCNEAL receiving stolen property, food stamps,
 28 and other government assistance from numerous customers in exchange for drugs. There
 are several conversations regarding money that is only accessed through a preloaded
 debit card and/or an ATM.

30. The stored web history shows daily activity from May 25, 2020, through
 his October arrest. Although the history showed approximately 31+ websites visited per

1 day (4316 sites over 135 days), there is no data between July 29th and August 3rd, 2020,
2 (the days preceding the death of Bradley Economou). Also of interest to investigators,
3 MCNEAL visited the Lewis County Jail Roster 201 times from June 14, 2020 until
4 October 7, 2020 (115 days); including within an hour and a half of MCNEAL's arrest.
5 Investigators believe MCNEAL was checking the jail register this often in order to see if
6 law enforcement had arrested any of his customers and/or who could possibly be working
7 as confidential sources for law enforcement.

8 **C. Jail Calls**

9 31. Shortly after MCNEAL was placed into custody he made several phone
10 calls to B.W., with whom he has fathered children. On October 9, 2020, at 4:48pm,
11 MCNEAL spoke to B.W. at phone number 360-442-1913, during which MCNEAL asks
12 B.W. to go into his "account" and "clear out mine"; indicating that MCNEAL wanted
13 B.W. to remove any data stored in a cloud type service. MCNEAL later clarified that
14 B.W. needed to log in through her phone, which was the same type of phone that
15 MCNEAL had. B.W. agreed to do so, and MCNEAL verbally gave her the password to
16 the account. MCNEAL told B.W. not to mention the email address associated with the
17 account as the call is being recorded and monitored.

18 32. In a subsequent phone call, on October 10, 2020, at 2:42pm, B.W. again
19 spoke to MCNEAL from the same x1913 number and told MCNEAL that she attempted
20 to login but needs access to MCNEAL's iPad as an account passcode or link was sent to
21 that device. MCNEAL responded by saying "you haven't done that yet?". MCNEAL
22 subsequently told B.W. that the iPad can be located at his cousin's residence.

23 33. During a later post-Miranda interview, on November 24, 2020, at
24 approximately 12:30pm, investigators asked B.W. about her involvement with
25 MCNEAL. Specifically, investigators asked her if MCNEAL ever asked her to do
26 anything for him. Initially the question was directed at whether B.W. gathered drug
27 proceeds to raise bail money for MCNEAL. B.W. responded that the only thing
28 MCNEAL had asked her to do was to go into his "account" and delete stored

1 information. B.W. stated that she did attempt to get into MCNEAL's "account" but
2 could not gain access to the account because she did not have access to his iPad, where an
3 account passcode or link had been sent. B.W. eventually stated that she gained access to
4 his "account" but that she changed her mind once inside the "account" because a family
5 member of hers had previously been arrested and charged with tampering with evidence
6 during a similar situation. Investigators noted that during this meeting B.W.'s phone was
7 an Apple iPhone.

8 34. On November 24, 2020, at 3:28pm following the above-mentioned
9 interview, MCNEAL called B.W. at the same x1913 number. B.W. immediately stated
10 that she had been contacted by law enforcement regarding a potential conspiracy charge,
11 MCNEAL interrupted her and stated that they were on a recorded line and to be cautious
12 about what she said. Shortly thereafter the phone call disconnected and MCNEAL
13 immediately called B.W. back. B.W. continues telling MCNEAL that law enforcement
14 questioned her about collecting drug proceeds for MCNEAL. B.W. clarified that she was
15 questioned about accessing MCNEAL's "iCloud account." B.W. specifically said that
16 officers stated, "they could see my IP address when I went to delete your iCloud," to
17 which MCNEAL acknowledged the failed attempt at deleting the iCloud account by
18 stating "well good job, because you didn't."

19 **III. MCNEAL'S iCloud Account**

20 35. According to information obtained from Apple on November 21, 2020,
21 MCNEAL registered for an iCloud account under the username
22 gooddealjohnmcneal@gmail.com. The registration information associated with this
23 account included the name "John McNeal," the telephone number 360-508-0839, and the
24 DSID – a unique identifier associated with a customer's iCloud account –
25 10998323040. As of November 21, 2020, this account remains active.

26 36. According to information obtained from a search of the iPhone 8 plus silver
27 64GB VZN-USA taken from MCNEAL during his arrest, done pursuant to a search
28

1 warrant, the telephone number 360-508-0839 was registered to MCNEAL and a device
2 with the IMEI number 356714087488322.

3 37. Since 2017, seven devices have been registered to MCNEAL'S Apple
4 iCloud account under the DSID 10998323040. Those seven devices are (1) an iPhone 8
5 Plus Red 64GB SPNT-USA with the IMEI number 356111091893789, registered on June
6 13, 2018; (2) an iPad wi-fi cell 32GB space gray VZ-USA, registered on December 19,
7 2018; (3) an iPhone 6S space gray 32GB SPR-USA, registered on March 20, 2019; (4) an
8 iPhone XR blue 64GB T-MO-USA, registered on March 29, 2019; (5) an iPhone XR
9 coral 64GB AT&T-USA, registered on October 1, 2019; (6) an iPhone 8 plus silver
10 64GB VZN-USA, with the IMEI number 356714087488322, registered on December 28,
11 2019; and (7) an iPhone XR white 64GB SPR-USA, registered on October 12, 2020.

12 38. Bradley Economou was discovered deceased on August 4, 2020. L.B.
13 delivered heroin to Bradley Economou on August 3, 2020. L.B. obtained the heroin she
14 delivered to Bradley Economou from MCNEAL on August 2 or 3, 2020. MCNEAL
15 accessed his Apple account both before and after this timeframe. For example,
16 MCNEAL's Apple account accessed the services MyApple ID and iForgot in July 2020
17 and September 2020. MCNEAL'S Apple account completed iTunes Music Store
18 transaction on both July 27, 2020 and August 8, 2020.

19 39. Apple provided law enforcement with MCNEAL'S iCloud activity for
20 October to November 2019. During this time period, MCNEAL'S iCloud account
21 cumulatively accessed the services Cloud Photo Library, iCloud Drive, Find my iPhone,
22 Backup, Contacts, Calendar, Notes, and Safari Browsing History over 15,000 times.

23 //

24 //

25 //

BACKGROUND ON APPLE ID AND ICLOUD⁶

40. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

41. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

42. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

43. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

44. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud can be utilized to transfer data from an old device to a new device, including data derived from device backups and third-party applications.

45. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device.

⁶ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “iCloud: iCloud storage and backup overview,” available at <https://support.apple.com/kb/PH12519>; and “iOS Security,” available at http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf.

1 For example, iCloud Mail enables a user to access Apple-provided email accounts on
2 multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream
3 can be used to store and manage images and videos taken from Apple devices, and
4 iCloud Photo Sharing allows the user to share those images and videos with other Apple
5 subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other
6 documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in
7 the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of
8 productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create,
9 store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a
10 user to keep website username and passwords, credit card information, and Wi-Fi
11 network information synchronized across multiple Apple devices.

12 46. Game Center, Apple's social gaming network, allows users of Apple
13 devices to play and share games with each other.

14 47. Find My iPhone allows owners of Apple devices to remotely identify and
15 track the location of, display a message on, and wipe the contents of those devices.

16 48. Location Services allows apps and websites to use information from
17 cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to
18 determine a user's approximate location.

19 49. App Store and iTunes Store are used to purchase and download digital
20 content. iOS apps can be purchased and downloaded through App Store on iOS devices,
21 or through iTunes Store on desktop and laptop computers running either Microsoft
22 Windows or Mac OS. Additional digital content, including music, movies, and television
23 shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop
24 computers running either Microsoft Windows or Mac OS.

25 50. Apple services are accessed through the use of an "Apple ID," an account
26 created during the setup of an Apple device or through the iTunes or iCloud services. A
27 single Apple ID can be linked to multiple Apple services and devices, serving as a central
28 authentication and syncing mechanism.

1 51. An Apple ID takes the form of the full email address submitted by the user
2 to create the account; it can later be changed. Users can submit an Apple-provided email
3 address (often ending in @icloud.com, @me.com, or @mac.com) or an email address
4 associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The
5 Apple ID can be used to access most Apple services (including iCloud, iMessage, and
6 FaceTime) only after the user accesses and responds to a “verification email” sent by
7 Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,”
8 and “notification” email addresses) can also be associated with an Apple ID by the user.

9 52. Apple captures information associated with the creation and use of an
10 Apple ID. During the creation of an Apple ID, the user must provide basic personal
11 information including the user’s full name, physical address, and telephone numbers.
12 The user may also provide means of payment for products offered by Apple. The
13 subscriber information and password associated with an Apple ID can be changed by the
14 user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition,
15 Apple captures the date on which the account was created, the length of service, records
16 of log-in times and durations, the types of service utilized, the status of the account
17 (including whether the account is inactive or closed), the methods used to connect to and
18 utilize the account, the Internet Protocol address (“IP address”) used to register and
19 access the account, and other log files that reflect usage of the account.

20 53. Additional information is captured by Apple in connection with the use of
21 an Apple ID to access certain services. For example, Apple maintains connection logs
22 with IP addresses that reflect a user’s sign-on activity for Apple services such as iTunes
23 Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on
24 Apple’s website. Apple also maintains records reflecting a user’s app purchases from
25 App Store and iTunes Store, “call invitation logs” for FaceTime calls, and “mail logs” for
26 activity over an Apple-provided email account. Records relating to the use of the Find
27 My iPhone service, including connection logs and requests to remotely lock or erase a
28 device, are also maintained by Apple.

1 54. Apple also maintains information about the devices associated with an
2 Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains
3 the user's IP address and identifiers such as the Integrated Circuit Card ID number
4 ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone
5 number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or
6 iMessage. Apple also may maintain records of other device identifiers, including the
7 Media Access Control address ("MAC address"), the unique device identifier ("UDID"),
8 and the serial number. In addition, information about a user's computer is captured when
9 iTunes is used on that computer to play content associated with an Apple ID, and
10 information about a user's web browser may be captured when used to access services
11 through icloud.com and apple.com. Apple also retains records related to communications
12 between users and Apple customer service, including communications regarding a
13 particular Apple device or service, and the repair history for a device.

14 55. Apple provides users with five gigabytes of free electronic space on iCloud,
15 and users can purchase additional storage space. That storage space, located on servers
16 controlled by Apple, may contain data associated with the use of iCloud-connected
17 services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My
18 Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and
19 other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network
20 information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS
21 device backups, which can contain a user's photos and videos, iMessages, Short Message
22 Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail
23 messages, call history, contacts, calendar events, reminders, notes, app data and settings,
24 and other data. Records and data associated with third-party apps may also be stored on
25 iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be
26 configured to regularly back up a user's instant messages on iCloud. Some of this data is
27 stored on Apple's servers in an encrypted form but can nonetheless be decrypted by
28 Apple.

1 56. In this case, I am investigating, among other things, the sale of illegal
2 narcotics including methamphetamine, heroin, and fentanyl laced counterfeit prescription
3 pills. In my training and experience, evidence of who was using an Apple ID and from
4 where, and evidence related to criminal activity of the kind described above, may be
5 found in the files and records described above. This evidence may establish the “who,
6 what, why, when, where, and how” of the criminal conduct under investigation, thus
7 enabling the United States to establish and prove each element or, alternatively, to
8 exclude the innocent from further suspicion.

9 57. The kinds of records maintained by Apple may help identify additional
10 transactions, identify the frequency that MCNEAL was deleting evidence from his phone,
11 and identify text messages discussing narcotic transactions. Apple’s records may also
12 help identify further information regarding the death of Bradley Economo, and the steps
13 taken by MCNEAL and others to destroy evidence of their involvement. For example,
14 the stored communications and files connected to an Apple ID may provide direct
15 evidence of the offenses under investigation. Based on my training and experience,
16 instant messages, emails, voicemails, photos, videos, and documents are often created
17 and used in furtherance of criminal activity, including to communicate and facilitate the
18 offenses under investigation.

19 58. Stored e-mails and chats not only may contain communications relating to
20 crimes, but also help identify the participants in those crimes. Address books and contact
21 lists may help identify and locate MCNEAL’s customers and identify any co-
22 conspirators, including the source of his methamphetamine, heroin, and fentanyl laced
23 counterfeit prescription pills. Documents may identify the scope of the criminal activity,
24 including transactional history. And calendar data may reveal the timing and extent of
25 criminal activity and other transactions. Search and browsing history can also be
26 extremely useful in identifying direct evidence of the crimes under investigation to the
27 extent the browsing history or search history might include searches and browsing history
28 related to MCNEALs continued criminal activity.

59. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account, which is particularly relevant to this investigation given the use of false identities. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

60. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

61. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal cryptocurrency wallet services used in furtherance of the crimes under investigation, services used to communicate with buyers or co-conspirators, or services used to store assets and cryptocurrencies used and obtained in furtherance of these crimes. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

62. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's

1 services. In my training and experience, such information may constitute evidence of the
2 crimes under investigation including information that can be used to identify the
3 account's user or users, an account user's assets, or applications and other services used
4 in furtherance of the crimes under investigation.

5 **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

6 63. I anticipate executing this warrant under the Electronic Communications
7 Privacy Act, in particular Title 18, United States Code, Sections 2703(a), (b)(1)(A), and
8 (c)(1)(A), by using the warrant to require Apple to disclose to the government copies of
9 the records and other information (including the content of communications) particularly
10 described in Section I of Attachment B. Upon receipt of the information described in
11 Section I of Attachment B, government-authorized persons will review that information
12 to locate the items described in Section II of Attachment B.

13 **CONCLUSION**

14 64. Based on the aforementioned factual information, I respectfully submit that
15 there is probable cause to believe that evidence, fruits, and instrumentalities of violations,
16 or attempted violations, of Distribution of, and Possession with Intent to Distribute,
17 Controlled Substances, in violation of 21 U.S.C. § 841(a)(1) (heroin and
18 methamphetamine); and Distribution of Counterfeit Drugs, in violation of 21 U.S.C. §
19 333(i)(3)(counterfeit Oxycodone pills containing fentanyl) may be located in the
20 SUBJECT ACCOUNT described in Attachment A.

21 //

22 //

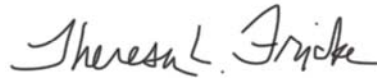
23 //

1 65. Based on the forgoing, I request that the Court issue the proposed search
2 warrant. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is
3 not required for the service or execution of this warrant. Because the warrant will be
4 served on Apple, who will then compile the requested records at a time convenient to it,
5 there exists reasonable cause to permit the execution of the requested warrant at any time
6 in the day or night.

7
8 

9 _____
10 COLIN FINE
11 Special Agent, DEA

12 Subscribed and sworn to before me this 18th day of December, 2020.

13
14 

15 _____
16 HON. THERESA L. FRICKE
17 United States Magistrate Judge
18
19
20
21
22
23
24
25
26
27
28

ATTACHMENT A
Property to Be Searched

This warrant applies to information associated with the Apple ID
goodealjohnmcneal@gmail.com (the “account”) that is stored at premises owned,
maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple
Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B
Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

1 c. The contents of all emails associated with the account from June 2020 to
2 the present, including stored or preserved copies of emails sent to and from the account
3 (including all draft emails and deleted emails), the source and destination addresses
4 associated with each email, the date and time at which each email was sent, the size and
5 length of each email, and the true and accurate header information including the actual IP
6 addresses of the sender and the recipient of the emails, and all attachments;

7 d. The contents of all instant messages associated with the account from June
8 2018 to the present, including stored or preserved copies of instant messages (including
9 iMessages, SMS messages, and MMS messages) sent to and from the account (including
10 all draft and deleted messages), the source and destination account or phone number
11 associated with each instant message, the date and time at which each instant message
12 was sent, the size and length of each instant message, the actual IP addresses of the
13 sender and the recipient of each instant message, and the media, if any, attached to each
14 instant message;

15 e. The contents of all files and other records stored on iCloud, including all
16 iOS device backups, all Apple and third-party app data, all files and other records related
17 to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud
18 Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and
19 bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes,
20 reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

21 f. All activity, connection, and transactional logs for the account (with
22 associated IP addresses including source port numbers), including FaceTime call
23 invitation logs, messaging and query logs (including iMessage, SMS, and MMS
24 messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases,
25 downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs,
26 sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My
27 Friends logs, logs associated with web-based access of Apple services (including all
28

1 associated identifiers), and logs associated with iOS device purchase, activation, and
 2 upgrades;

3 g. All records and information regarding locations where the account or
 4 devices associated with the account were accessed, including all data stored in connection
 5 with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

6 h. All records pertaining to the types of service used;

7 i. All records pertaining to communications between Apple and any person
 8 regarding the account, including contacts with support services and records of actions
 9 taken; and

10 j. All files, keys, or other information necessary to decrypt any data produced
 11 in an encrypted form, when available to Apple (including, but not limited to, the
 12 keybag.txt and fileinfolist.txt files).

13 The Provider is hereby ordered to disclose the above information to the
 14 government within 14 days of service of this warrant.

15 **II. Information to be seized by the government**

16 All information described above in Section I that constitutes fruits, evidence and
 17 instrumentalities of violations of Distribution of, and Possession with Intent to Distribute,
 18 Controlled Substances, in violation of 21 U.S.C. § 841(a)(1) (heroin and
 19 methamphetamine); Distribution of Counterfeit Drugs, in violation of 21 U.S.C. §
 20 333(i)(3)(Counterfeit Oxycodone pills containing fentanyl); (collectively the “Subject
 21 Offenses”), involving JOHN MCNEAL JR. since June 2020, including, for each
 22 username identified on Attachment A, information pertaining to the following matters:

23 a. Images and video recordings of narcotics, currency, firearms and
 24 other weapons, suspected criminal activity, and the user of the account of coconspirators,
 25 including any embedded GPS data associated with such images or recordings;

26 b. Evidence of communications or correspondence related to the
 27 Subject Offenses, including email, text messages, instant messages, WhatsApp calls and
 28

1 | messages, social media messages and posts, audio and video recordings, log files, and
2 | related databases;

3 | c. Records and data related to the identification of individuals
4 | committing the Subject Offenses;

5 | d. Records and data that may reveal the identities of or relationships
6 | between coconspirators;

7 | e. Records, receipts, notes, ledgers, and other documents relating to the
8 | distribution of controlled substances, firearms and other weapons, and communications
9 | between coconspirators;

10 | f. Internet-based multimedia messaging services or applications, such
11 | as WhatsApp and Facebook, used for communications and their contents if related to the
12 | Subject Offenses; and

13 | g. Records and data that may identify assets (such as bank accounts,
14 | wire-transfer records, digital currency accounts, personal property, and real estate) that
15 | may represent proceeds of the Subject Offenses or that are traceable to such proceeds.

16 | h. Evidence of who used, owned, or controlled the SUBJECT
17 | ACCOUNT, including records and data that may reveal the current or past location of the
18 | individual or individuals using the SUBJECT ACCOUNT; assigned number and
19 | identifying telephone serial number (ESN, MIN, IMSI, or IMEI); logs; stored lists of
20 | received, sent, or missed calls; phonebooks; address books; saved usernames and
21 | passwords; and documents.

22 | i. Records and data that may identify any alias names or usernames of
23 | those who exercise in any way any dominion or control over the SUBJECT ACCOUNT,
24 | as well as records and information that may reveal the true identities of these individuals.

25 | j. Passwords, encryption keys, and other access devices that may be
26 | necessary to access the SUBJECT ACCOUNT or to access communication and financial
27 | accounts associated with the devices or the device users.

1 k. Evidence of the attachment to the SUBJECT ACCOUNT of other
2 storage devices or similar containers for electronic evidence.

3 l. Any other electronically stored information from the SUBJECT
4 ACCOUNT necessary to understand how the device and/or account was used, the
5 purpose for which it was used, and when.

6 m. Evidence of Internet Protocol (IP) addresses used.

7 n. Records of internet activity, including firewall logs, caches, browser
8 history and cookies, bookmarked or "favorite" webpages, search terms the user entered
9 into any internet search engine, and records of user-typed web addresses. As used above,
10 the terms "records" and "information" include all the foregoing items of evidence in
11 whatever form and by whatever means they may have been created or stored, including
12 any form of computer or electronic storage (such as flash memory or other media that can
13 store data) and any photographic form.

14 o. Evidence indicating the subscriber's state of mind as it relates to the
15 crime under investigation; and

16 p. Evidence that my identify any co-conspirators or aiders and abettors
17 including records that help reveal their whereabouts.

18 This warrant authorizes a review of electronic storage media and
19 electronically stored information seized or copied pursuant to this warrant in order to
20 locate evidence, fruits, and instrumentalities described in this warrant. This review may
21 be conducted by any government personnel assisting in the investigation, who may
22 include, in addition to law enforcement officers and agents, attorneys for the government,
23 attorney support staff, and technical experts. Pursuant to this warrant, the DEA may
24 deliver a complete copy of the seized or copied electronic data to the custody and control
25 of attorneys for the government and their support staff for their independent review.
26
27
28

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT
TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by
the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the
information contained in this certification is true and correct. I am employed by Apple,
Inc. ("Apple"), and my title is _____. I am qualified to
authenticate the records attached hereto because I am familiar with how the records were
created, managed, stored, and retrieved. I state that the records attached hereto are true
duplicates of the original records in the custody of Apple. The attached records consist of
_____ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I
further state that:

a. all records attached to this certificate were made at or near the time of the
occurrence of the matter set forth by, or from information transmitted by, a person with
knowledge of those matters, they were kept in the ordinary course of the regularly
conducted business activity of Apple, and they were made by Apple as a regular practice;
and

b. such records were generated by Apple's electronic process or system that
produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage
medium(s), or file(s) in the custody of Apple in a manner to ensure that they are true
duplicates of the original records; and

2. the process or system is regularly verified by Apple, and at all times
pertinent to the records certified here the process and system functioned properly and
normally.

I further state that this certification is intended to satisfy Rules 902(11) and
902(13) of the Federal Rules of Evidence.

Date: _____

Signature: _____